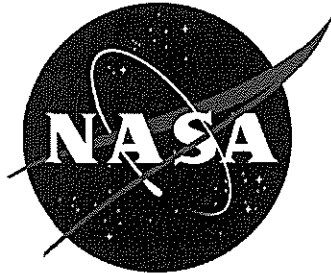


NASA Information Technology Requirement



NITR 2810-22

Effective Date: January 7, 2009

Expiration Date: May 16, 2011

Media Protection Policy and Procedures

Responsible Office: Office of the Chief Information Officer

Table of Contents

Change History

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents
- P.5 Measurement and Verification
- P.6 Cancellation

1.0 REQUIREMENT

- 1.1 Media Protection Policy
- 1.2 Procedures

APPENDIX A. Descriptions

APPENDIX B. Acronyms

Distribution

NODIS

NITR-2810-22, Media Protection Policy and Procedures

Change Number	Date	Change Description

PREFACE

P.1 PURPOSE

- a. To provide the NASA media protection policy and procedures for NASA information and information systems to meet the requirements of the National Institute of Standards and Technology (NIST) and the Agency mission.

P.2 APPLICABILITY

- a. This NITR applies to unclassified information and information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

P.3 AUTHORITY

- a. Reference Paragraph P.3, NPR 2810.1A.

P.4 APPLICABLE DOCUMENTS

- a. NPR 2810.1A, Security of Information Technology.
- b. NPR 1382.1, NASA Privacy Procedural Requirements.
- c. NPR 1600.1, NASA Security Program Procedural Requirements.
- d. NPR 1441.1D, NASA Records Retention Schedules.
- e. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- f. NIST SP 800-100, Information Security Handbook: A Guide to Managers.
- g. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- h. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- i. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.
- j. NIST SP 800-88, Guidelines for Media Sanitization.

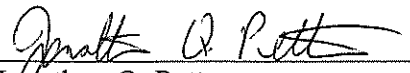
P.5 MEASUREMENT AND VERIFICATION

- a. Annual certification of the Agency Common Security Control, MP-1 Media Protection Policy and Procedures.

b. Annual assessment of the Agency MP-1 common security control by the Information System Owner (ISO) as part of the system Continuous Monitoring requirement.

P.6 CANCELLATION

a. The next version of NPR 2810.1 cancels this NITR.


Jonathan Q. Pettus
NASA Chief Information Officer

1-7-09
Date

1.0 REQUIREMENT

1.1 Media Protection Policy

1.1.1. The NASA media protection policy shall be consistent with applicable laws, Executive Orders, directives, regulations and guidance. The objective is to assure effective media protection and controls to prevent loss or unauthorized access to NASA information or information systems.

1.1.2. All NASA information systems shall implement the current NIST 800-53 media protection security control requirements.

1.1.3. NASA information systems, and/or systems that process or store NASA data, shall be kept up-to-date with the latest patches and anti-virus signatures.

1.1.4. Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm).

1.1.5. Computing devices include portable/mobile devices and non-mobile devices.

1.1.5.1. Portable and mobile devices include laptops, Personal Digital Assistants (PDAs), cellular telephones, and other portable or mobile devices with information storage capability.

1.1.5.2. End user computing and storage devices fall into one of the following categories:

a. NASA provided desktop and laptop computers or (PDAs, e.g., Blackberry devices). These are computers or PDAs operating in NASA IP space that are NASA purchased and owned or have been contracted for use by NASA employees and/or support contractors, (e.g. Outsourcing Desktop Initiative NASA (ODIN) contract).

b. Personally owned, a NASA contractor owned, or a NASA external activity owned (e.g. university) desktop or laptop computers or PDAs used to connect to NASA systems and networks for telecommuting purposes; where the user has full responsibility for the administration of the device's security controls.

c. Third-party desktop or laptop computers. These devices are normally found in telecommuting centers, libraries and public kiosks such as those located in airports. Such devices are open and available to the general public and the user has very limited or no responsibility for the administration of the device's security controls.

d. Removable media which typically consists of portable devices that can be used to copy, save, store and/or move data from one system to another. Media devices come in various forms that include, but are not limited to, USB drives, flash drives or cards, read/write CDs, memory cards, external hard drives and PDA storage cards.

1.1.6. Information Security

1.1.6.1. Every effort shall be taken to ensure the confidentiality, integrity and availability of NASA information. While flexibility is given to end users to process, store or transmit NASA information using personally owned devices or in some situations using third-party devices, certain types of NASA Sensitive but Unclassified (SBU) data shall not be processed, stored or transmitted on personally owned or third-party devices at any time. These data types include:

- a. National security or classified data.
- b. Controlled under International Traffic Arms in Regulations (ITAR).
- c. Controlled under the Export Administration Regulations (EAR).

1.1.6.2. Personally Identifiable Information (PII) shall not be stored on personally owned devices or on third-party devices except for limited, approved exceptions. In certain situations, third-party devices located in NASA authorized telecommuting centers may be used to process and transmit (but not store) PII if authorized in writing by the individual's supervisor. An example of when third-party telecommuting devices may be used to process and transmit PII is during the execution of the organization's business continuity plan (BCP) or when users must carry out their job responsibilities at an authorized NASA alternate processing facility.

1.1.6.3. Sensitive information and Sensitive but Unclassified (SBU) information:

a. Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987, Public Law 100-235).

b. SBU information is information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes. Information that meets the "Sensitive Information" criteria in above paragraph shall be designated as SBU.

1.1.6.4. The requirements and procedures for identifying and designating SBU information, marking, storing, transmitting, and destroying SBU information are specified in NPR 1600.1, NASA Security Program Procedural Requirements.

1.1.6.5. SBU information shall not be disseminated in any manner - orally, visually, or electronically to unauthorized personnel.

1.1.6.6. Access to media containing non-public information shall be restricted to authorized individuals and includes digital media with information storage capability and non-digital media. (Non-public information is the "private" NASA information and information systems to which access is restricted and appropriately controlled through a formal process).

1.1.6.7. Access to SBU information is based on "need-to-know" as determined by the holder of the information. Reasonable precautions should be taken to prevent access to SBU information by persons who do not require the information to perform their jobs. Where there is uncertainty as to a person's need-to-know, the holder of the information shall request dissemination instructions from their next-level supervisor or the originator of the information.

1.1.6.8. SBU information shall be destroyed when it is no longer needed and in accordance with NPR 1441.1, NASA Records Retention Schedules.

1.1.6.9. SBU information downloaded from any NASA information system shall be erased and/or destroyed within 90 days unless formal justification is provided for retention and approved by the originator of the data. This includes digital as well as non-digital media.

1.1.6.10. Laptop computers and other media containing SBU information shall be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure.

1.1.6.11. Portable and mobile media devices, including flash/thumb drives, shall be encrypted in accordance with the NASA data at rest encryption policy and procedures using FIPS 140-2 compliant and validated encryption.

1.1.6.12. For High security category information systems, all information system media and output shall be labeled except for that information determined to be in the public domain or is publicly releasable.

1.1.7. Incident Reporting

1.1.7.1. A PII breach occurs when the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an authorized purpose have access or potential access to PII in usable form, whether physical or electronic. A PII breach or suspected PII breach shall be reported immediately upon discovery as an information security incident.

1.1.7.2. Information security incidents or suspected information security incidents, such as loss of a device with NASA information, a PII breach, or the compromise of NASA information, shall be immediately reported to the NASA Security Operations Center (SOC) through the SOC Incident Response help desk. The Center Information Technology Security Manager (ITSM) shall be notified in accordance with SOC incident response procedures.

1.1.8. Media Storage

1.1.8.1. For removable media (paragraph 1.1.5.2.d), NASA personnel and contractors shall:

- a. Not use personally owned removable media devices in government-owned systems.
- b. Not use government owned removable media devices on personal machines or machines that do not belong to the Agency, department or organization.
- c. Not put unknown removable media devices into ANY system.

1.1.8.2. For media storage of Moderate or High security category information systems:

- a. Media with information considered critical, e.g. mission operations, needed for system restoration, security audits, investigations, etc. shall be identified as such, secured in a locked container, and with specifically defined access authorizations and controls.
- b. If data at rest encryption is used on media which stores information considered critical, cryptographic key management shall be established and maintained that provides the required protection and assures the availability of the information in the event of cryptographic key loss by users.

1.1.9. Media Transportation

1.1.9.1. NASA non-public data shall be protected when transported outside of NASA controlled areas and, for SBU, in accordance with the requirements specified in NPR 1600.1, NASA Security Program Procedural Requirements.

1.1.9.2. For High security category information system media with non-public data and for Moderate security category media that is needed for system backup/recovery or that has specific controls, e.g. SBU – Export Administrative Regulation; SBU – NASA Developed Software, the following controls and criteria shall be used when transported outside the controlled area:

- a. Encrypt digital media with FIPS 140-2 compliant and validated encryption.
- b. Use a locked container, e.g., locked briefcase, for non-digital media or portable media devices such as CDs or DVDs.
- c. An ISO designated custodian/courier, registered mail, or an authorized delivery service with an accountable tracking system and manifest included in the shipment
- d. Maintain a formal log identifying the media, custodian, time provided to the custodian, and the destination.

1.1.10. Media Sanitization

1.1.10.1. Digital Media Sanitization shall use the procedures, processes, methods, mechanisms and tools to clear/purge or destroy data for the various media type as specified in the ITS-SOP-0035, *Digital Media Sanitization*.

1.1.10.2. For Moderate and High security category information systems, NASA shall implement the minimum digital media sanitization requirements and procedures of NIST SP 800-88. To meet the minimum sanitization requirements, media sanitization personnel may need to use the practices and processes identified in DoD Sanitization Standard 5520.22-M, NASA Storage Device Destruction Guidance, and other industry and Government best practices. (See ITS-SOP-0035)

1.1.10.3. For High security category information systems:

- a. A record of media sanitation shall be maintained using the “Media Sanitization Record Form” included in the ITS-SOP-0035.
- b. Tests of the sanitization equipment used shall be conducted at least quarterly to ensure they are performing as intended.

1.1.10.4. Non-digital SBU media shall be sanitized/destroyed in accordance with the requirements specified in NPR 1600.1, NASA Security Program Procedural Requirements.

1.1.10.5. Media containing federal records shall not be sanitized/destroyed unless in compliance with NPR 1441.1, NASA Records Retention Schedules.

1.2 Procedures

1.2.1. NASA employees, detailees, contractors, consultants and others to whom access is granted shall:

- a. Be aware of, and comply with, the safeguarding requirements for SBU information as specified in this policy.
- b. Be responsible for reporting any violation of this policy to their supervisor or appropriate personnel.

- c. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding SBU and other sensitive information.
- d. Be aware that divulging information without proper authority could result in administrative or disciplinary action.
- e. Report to the SOC any suspected or actual PII breaches within one hour of discovery (see paragraph 1.1.7 above).
- f. Comply with the NASA removable media requirements (see paragraph 1.1.8.1).

1.2.2 NASA Supervisors and Managers shall:

- a. Be aware of and comply with the safeguarding requirements for SBU information as outlined in this policy.
- b. Ensure that only authorized employees have access to SBU information.
- c. Annually, and more often as necessary, inform their employees of the need to protect SBU information and the requirement to receive approval prior to SBU information being removed from agency property.
- d. Be responsible for reporting any violation of this policy to the appropriate personnel.
- e. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

1.2.3 The ISO shall:

- a. Assure implementation of the above Agency Media Protections policies for their information system and stored information.
- b. Document the system Media Protections requirements and procedures in the System Security Plan (SSP).

1.2.4 The Senior Agency Information Security Officer (SAISO) shall:

- a. Annually review, and update as required, the Agency media protection policy as part of the annual review of the CP-1 Agency Common Control providing management oversight to ensure policy currency and compliance.
- b. Annually certify the CP-1 Agency Common Control to ensure it satisfies the purpose, scope, and compliance requirements for media protection.
- c. Ensure the Agency data-at-rest-encryption requirements are established for encryption of NASA portable and mobile media devices.

APPENDIX A. Descriptions

Term	Definition
Authorizing Official	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200 adapted]
Certification	A confirmation in formal documentation that an accepted standard has been met.
Common Control	A security control that is inherited by an information system
Continuous Monitoring	Refers to a phase of the Certification and Accreditation Process of Information Systems. It consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.
Data	Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, such as computerized databases, paper microfilm, tapes, disk, memory chips, RAM, ROM, microfiche, communication lines, and display terminals
Data at Rest	Data at rest is a term that is sometimes used to refer to all data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at rest can be archival or reference files that are changed rarely or never; data at rest can also be data that is subject to regular but not constant change. Examples include vital corporate files stored on the hard drive of an employee's notebook computer, files on an external backup medium, files on the servers of a storage area network (SAN), or files on the servers of an offsite backup service provider.
Encryption	The translation of data into a form that is unintelligible without a deciphering mechanism
Hybrid Security	A security control that is part common control and part system-

Control	specific control
Information System Owner	An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. [OMB Circular A-130, Appendix III] (Also referred to as IT System)
Information Technology	Any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation [FIPS 199]
IT System	See Information System
Non-Public	See "Private" NASA IT System
Personally Identifiable Information	PII is any information about an individual maintained by an agency which can be used to distinguish or trace an individual's identity. Some information that is considered to be PII is available in public sources such as telephone books, public websites, university listings, etc. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. In contrast, Protected PII is defined as a social security number as a stand alone, or an individual's first name or first initial and last name in combination with any one or more types of the following information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, etc. This information may be in the form of paper, electronic or any other media format.

"Private" NASA IT System	Those NASA IT systems to which access is restricted and appropriately controlled through a formal process. Granting of access is contingent upon a favorable security background investigation commensurate with the risk level of the system
"Public" NASA IT System	Those NASA IT systems to which access is unrestricted
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the Nation. [FIPS 199 as amended by NIST SP 800-53]
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Sensitive but Unclassified	Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes. Also see "Sensitive Information"

<p>Sensitive But Unclassified (SBU) Controlled Information/Material (NPR 1600.1)</p>	<p>Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations:</p> <ul style="list-style-type: none"> (1) ITAR - International Traffic in Arms Regulations (2) EAR - Export Administration Regulations (3) MCTL - Militarily Critical Technologies List (4) FAR - Federal Acquisition Regulations (5) Privacy Act (6) Proprietary (7) FOIA - Freedom of Information Act (8) UCNI - Unclassified Controlled Nuclear Information (9) NASA Developed Software (10) Scientific and Technical Information (STI) (11) Source Selection and Bid and Proposal Information (12) Inventions
<p>Sensitive Information</p>	<p>Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987, Public Law 100-235)</p>

APPENDIX B. Acronyms

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FNMS	Foreign National Management System
ISO	Information System Owner
ITSM	Information Technology Security Manager
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
SAISO	Senior Agency Information Security Officer
SBU	Sensitive but Unclassified
SP	Special Publication
SSP	System Security Plan